PORTAL

USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

scrambling AND "substitution table" SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used **scrambling** AND **substitution table** Found **340** of **196,760**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Advances in design-for-testability methods: Secure scan: a design-for-test architecture for crypto chips

Bo Yang, Kaijie Wu, Ramesh Karri

June 2005 **Proceedings of the 42nd annual conference on Design automation DAC '05**

Publisher: ACM Press

Full text available: pdf(234.65 KB) Additional Information: full citation, abstract, references, index terms

Scan-based Design-for-Test (DFT) is a powerful testing scheme, but it can be used to retrieve the secrets stored in a crypto chip thus compromising its security. On one hand, sacrificing security for testability by using traditional scan-based DFT restricts its use in privacy sensitive applications. On the other hand, sacrificing testability for security by abandoning scan-based DFT hurts product quality. The security of a crypto chip comes from the small secret key stored in a few registers and ...

Keywords: crypto hardware, scan-based DFT, security, testability

2 Algorithm 823: Implementing scrambled digital sequences

Hee Sun Hong, Fred J. Hickernell

June 2003 **ACM Transactions on Mathematical Software (TOMS),** Volume 29 Issue 2

Publisher: ACM Press

Full text available: pdf(215.42 KB) Additional Information: full citation, abstract, references, citings, index terms

Random scrambling of deterministic (t, m, s)-nets and (t, s)-sequences eliminates their inherent bias while retaining their low-discrepancy properties. This article describes an implementation of two types of random scrambling, one proposed by Owen and another proposed by Faure and Tezuka. The four different constructions of digital sequences implemented are those proposed by Sobol', Faure, Niederreiter, and Niederreiter and Xing. Because the random scrambling ...

Keywords: Scrambling, digital net

3 Efficient frequency domain video scrambling for content access control

Wenjun Zeng, Shawmin Lei

October 1999 **Proceedings of the seventh ACM international conference on Multimedia (Part 1) MULTIMEDIA '99**

Publisher: ACM Press
Full text available: pdf(1.65 MB) Additional Information: full citation, abstract, references, index terms

Multimedia data security is very important for multimedia commerce on the Internet such as video-on-demand and real-time video multicast. Traditional cryptographic algorithms for data security are often not fast enough to process the vast amount of data generated by the multimedia applications to meet the real-time constraints. This paper presents a joint encryption and compression framework in which video data are scrambled efficiently in the frequency domain by employing selective bit scr ...

Keywords: compression, content access control, multimedia commerce, multimedia encryption, multimedia security, selective encryption, video scrambling

4 Cost-based query scrambling for initial delays
Tolga Urhan, Michael J. Franklin, Laurent Amsaleg
June 1998 **ACM SIGMOD Record , Proceedings of the 1998 ACM SIGMOD international conference on Management of data SIGMOD '98**, Volume 27 Issue 2
Publisher: ACM Press
Full text available: pdf(1.81 MB) Additional Information: full citation, abstract, references, citings, index terms

Remote data access from disparate sources across a wide-area network such as the Internet is problematic due to the unpredictable nature of the communications medium and the lack of knowledge about the load and potential delays at remote sites. Traditional, static, query processing approaches break down in this environment because they are unable to adapt in response to unexpected delays. Query scrambling has been proposed to address this problem. Scrambling modifies query execution plans o ...

5 Power modeling and optimization for embedded systems: Energy-efficient data scrambling on memory-processor interfaces
Luca Benini, Angelo Galati, Alberto Macii, Enrico Macii, Massimo Poncino
August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design ISLPED '03**
Publisher: ACM Press
Full text available: pdf(147.39 KB) Additional Information: full citation, abstract, references, index terms

Crypto-processors are prone to security attacks based on the observation of their power consumption profile. We propose new techniques for increasing the non-determinism of such profile, which rely on the idea of introducing randomness in the bus data transfers. This is achieved by combining data scrambling with energy-efficient bus encoding, thus providing high information protection at no energy cost.Results on a set of bus traces originated by real-life applications demonstrate the applicabil ...

Keywords: bus encoding, data scrambling, power attacks

6 Speech & phonology: Towards a proper linguistic and computational treatment of scrambling: an analysis of Japanese
Sandiway Fong
August 1994 **Proceedings of the 15th conference on Computational linguistics - Volume 2**
Publisher: Association for Computational Linguistics
Full text available: pdf(424.69 KB) Additional Information: full citation, abstract, references

This paper describes how recent linguistic results in explaining Japanese short and long distance scrambling can be directly incorporated into an existing principles-and-parameters-based parser with only trivial modifications. The fact that this is realizable on a parser originally designed for a fixed-word-order language, together with the fact that Japanese scrambling is complex, attests to the high degree of crosslinguistic generalization present in the theory.

7 Long-distance scrambling and tree adjoining grammars
Tilman Becker, Aravind K. Joshi, Owen Rambow
April 1991 **Proceedings of the fifth conference on European chapter of the Association for Computational Linguistics**
Publisher: Association for Computational Linguistics
Full text available: pdf(604.38 KB) Publisher Site
Additional Information: full citation, references, citings

8 Student session: Mapping scrambled Korean sentences into English using synchronous tags
Hyun S. Park
June 1995 **Proceedings of the 33rd annual meeting on Association for Computational Linguistics**
Publisher: Association for Computational Linguistics
Full text available: pdf(272.73 KB) Publisher Site
Additional Information: full citation, abstract, references

Synchronous Tree Adjoining Grammars can be used for Machine Translation. However, translating a free order language such as Korean to English is complicated. I present a mechanism to translate scrambled Korean sentences into English by combining the concepts of Multi-Component TAGs (MC-TAGs) and Synchronous TAGs (STAGs).

9 Demonstration session 1: A scrambling method based on disturbance of motion vector
Bodo Yann, Laurent Nathalie, Dugelay Jean-Luc
December 2002 **Proceedings of the tenth ACM international conference on Multimedia MULTIMEDIA '02**
Publisher: ACM Press
Full text available: pdf(209.68 KB) Additional Information: full citation, abstract, references

Multimedia data security is very important for multimedia commerce on the Internet such as "pay-per-view" services. Thus, watermarking algorithms for data security appear. These algorithms describe methods and technologies that allow information to be hidden, for example a number or text, into a media, such as images, video, audio files... In this paper, we propose a new application of watermarking based on a scrambling process. In this application, we develop a waterscrambling technique in whic ...

Keywords: motion vector, watermarking, waterscrambling

10 Session: Chinese numbers, MIX, scrambling, and range concatenation grammars
Pierre Boullier
June 1999 **Proceedings of the ninth conference on European chapter of the Association for Computational Linguistics**
Publisher: Association for Computational Linguistics
Full text available: pdf(747.58 KB) Publisher Site
Additional Information: full citation, abstract, references, citings

The notion of mild context-sensitivity was formulated in an attempt to express the formal power which is both necessary and sufficient to define the syntax of natural languages.

However, some linguistic phenomena such as Chinese numbers and German word scrambling lie beyond the realm of mildly context-sensitive formalisms. On the other hand, the class of range concatenation grammars provides added power w.r.t. mildly context-sensitive grammars while keeping a polynomial parse time behavior. In t ...

11 Scrambled storage for parallel memory systems □
D. Lee
May 1988 **ACM SIGARCH Computer Architecture News , Proceedings of the 15th Annual International Symposium on Computer architecture ISCA '88**, Volume 16 Issue 2
Publisher: IEEE Computer Society Press, ACM Press
Full text available: pdf(806.08 KB) Additional Information: full citation, abstract, references, citings, index terms

A scrambled storage scheme is proposed for storing arrays of NXN elements in N = 2n parallel memory modules to allow conflict-free access to various array partitions. It is shown that the scheme allows conflict-free access to rows, columns, square blocks, and distributed blocks of stored arrays. An alternative way of achieving the desired accessibility would use Budnik and Kuck's nonuniform skewed storage [3]; in this c ...

12 Variance with alternative scramblings of digital nets □
Art B. Owen
October 2003 **ACM Transactions on Modeling and Computer Simulation (TOMACS)**, Volume 13 Issue 4
Publisher: ACM Press
Full text available: pdf(170.32 KB) Additional Information: full citation, abstract, references, citings, index terms

There have been many proposals for randomizations of digital nets. Some of those proposals greatly reduce the computational burden of random scrambling. This article compares the sampling variance under different scrambling methods. Some scrambling methods adversely affect the variance, even to the extent of deteriorating the rate at which variance converges to zero. Surprisingly, a new scramble proposed here, has the effect of improving the rate at which the variance converges to zero, but so f ...

Keywords: Derandomization, quasi-Monte Carlo, randomization

13 Cognitive factors can influence self-motion perception (vection) in virtual reality □
Bernhard E. Riecke, Jörg Schulte-Pelkum, Marios N. Avraamides, Markus Von Der Heyde, Heinrich H. Bülthoff
July 2006 **ACM Transactions on Applied Perception (TAP)**, Volume 3 Issue 3
Publisher: ACM Press
Full text available: pdf(640.31 KB) Additional Information: full citation, abstract, references, index terms

Research on self-motion perception and simulation has traditionally focused on the contribution of physical stimulus properties ("bottom-up factors") using abstract stimuli. Here, we demonstrate that cognitive ("top-down") mechanisms like ecological relevance and presence evoked by a virtual environment can also enhance visually induced self-motion illusions (vection). In two experiments, naive observers were asked to rate presence and the onset, intensity, and convincing ...

Keywords: Ego--motion simulation, psychophysics, spatial orientation, spatial presence, vection, virtual reality

14 □
Learning response time for WebSources using query feedback and application in

query optimization
Jean-Robert Gruser, Louiqa Raschid, Vladimir Zadorozhny, Tao Zhan
March 2000 **The VLDB Journal — The International Journal on Very Large Data Bases**, Volume 9 Issue 1
Publisher: Springer-Verlag New York, Inc.
Full text available: pdf(625.36 KB) Additional Information: full citation, abstract, citings, index terms

The rapid growth of the Internet and support for interoperability protocols has increased the number of Web accessible sources, WebSources. Current wrapper mediator architectures need to be extended with a wrapper cost model (WCM) for WebSources that can estimate the response time (delays) to access sources as well as other relevant statistics. In this paper, we present a Web prediction tool (WebPT), a tool that is based on learning using query feedback from WebSources. The WebPT uses dimensions ...

Keywords: Data-intensive applications on the Web, Query languages and systems for Web data

15 Papers: virtual environments: Scene consistency and spatial presence increase the sensation of self-motion in virtual reality □
Bernhard E. Riecke, Jörg Schulte-Pelkum, Marios N. Avraamides, Markus von der Heyde, Heinrich H. Bülthoff
August 2005 **Proceedings of the 2nd symposium on Applied perception in graphics and visualization APGV '05**
Publisher: ACM Press
Full text available: pdf(517.68 KB) Additional Information: full citation, abstract, references, citings, index terms

The illusion of self-motion induced by moving visual stimuli ("vection") has typically been attributed to low-level, bottom-up perceptual processes. Therefore, past research has focused primarily on examining how physical parameters of the visual stimulus (contrast, number of vertical edges etc.) affect vection. Here, we investigated whether higher-level cognitive and top-down processes - namely global scene consistency and spatial presence - also contribute to the illusion. These factors were i ...

Keywords: ego-motion simulation, human factors, psychophysics, spatial orientation, spatial presence, vection, virtual reality

16 The isomorphism conjecture fails relative to a random oracle □
Stuart A. Kurtz, Stephen R. Mahaney, James S. Royer
March 1995 **Journal of the ACM (JACM)**, Volume 42 Issue 2
Publisher: ACM Press
Full text available: pdf(1.38 MB) Additional Information: full citation, references, citings, index terms, review

Keywords: conjecture, isomorphism, randomness

17 The ismorphism conjecture fails relative to a random oracle □
S. A. Kurtz, S. R. Mahaney, J. S. Royer
February 1989 **Proceedings of the twenty-first annual ACM symposium on Theory of computing STOC '89**
Publisher: ACM Press
Full text available: Additional Information: full citation, abstract, references, citings, index

pdf(1.09 MB) terms

Berman and Hartmanis [BH77] conjectured that there is a polynomial-time computable isomorphism between any two languages m-complete ("Karp" complete) for NP. Joseph and Young [JY85] discovered a structurally defined class of NP-complete sets and conjectured that certain of these sets (the Kk*f*'s) are not isomorphic to the standard NP-complete sets for some one-way functions *f*. These two conjectures cannot both b ...

18 Visual perception: Categorization of natural scenes: local vs. global information □

Julia Vogel, Adrian Schwaninger, Christian Wallraven, Heinrich H. Bülthoff

July 2006 **Proceedings of the 3rd symposium on Applied perception in graphics and visualization APGV '06**

Publisher: ACM Press

Full text available: pdf(6.95 MB) Additional Information: full citation, abstract, references, index terms

Understanding the robustness and rapidness of human scene categorization has been a focus of investigation in the cognitive sciences over the last decades. At the same time, progress in the area of image understanding has prompted computer vision researchers to design computational systems that are capable of automatic scene categorization. Despite these efforts, a framework describing the processes underlying human scene categorization that would enable efficient computer vision systems is stil ...

Keywords: computational modeling, gist, global configural information, local region-based information, scene classification, scene perception, semantic modeling

19 Verification and security: Policy-hiding access control in open environment □

Jiangtao Li, Ninghui Li

July 2005 **Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing PODC '05**

Publisher: ACM Press

Full text available: pdf(247.72 KB) Additional Information: full citation, abstract, references, citings, index terms

In trust management and attribute-based access control systems, access control decisions are based on the attributes (rather than the identity) of the requester: Access is granted if Alice's attributes in her certificates satisfy Bob's access control policy. In this paper, we develop a policy-hiding access control scheme that protects both sensitive attributes and sensitive policies. That is, Bob can decide whether Alice's certified attribute values satisfy Bob's policy, without Bob learning any ...

Keywords: access control, automated trust negotiation, cryptographic commitment, cryptographic protocol, digital credentials, evaluation, privacy, secure function

20 Short papers session 1: Low complexity controllable scrambler/descrambler for H.264/AVC in compressed domain □

Ho-Jae Lee, Jeho Nam

October 2006 **Proceedings of the 14th annual ACM international conference on Multimedia MULTIMEDIA '06**

Publisher: ACM Press

Full text available: pdf(668.13 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we present a novel algorithm that scrambles and descrambles a H.264/AVC video element stream. In particular, the proposed method selectively exploits the unique characteristics of H.264/AVC video coding standard. Specifically, we manipulate DCT coefficients and CABAC initialization table, to secure the visual content of H.264/AVC video. This new algorithm is light-weight and able to support the level of security (scrambling strength) as well. Extensive experimental results indicat ...

Keywords: AVC, CABAC, H.264, encryption, scramble, security

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Tuesday, January 16, 2007

Hide?	Set Name	Query	Hit Count
		DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR	
□	L48	l42 and (partial near3 (scrambl$8 or encrypt$5))	55
□	L47	l44 and (random near2 position)	0
□	L46	L45 and (random near4 position)	0
□	L45	L42 and (encrypt$8 and substitution)	90
□	L44	L42 and (scrambl$8 and substitution)	53
□	L43	L42 and (scrambl$8 same substitution)	3
□	L42	380/200,210,230,239.ccls.	951
□	L41	L40	0
□	L40	(mpeg same scarmbl$7 same header)	0
□	L39	((mpeg same scrambl$7 same header) same partial)	2
□	L38	((mpeg same scrambl$7 same header) and (s near2 box or (substitution near2 box)))	0
□	L37	((mpeg same scrambl$7) and header$7 and (s near2 box or (substitution near2 box)))	1
□	L36	(((scrambl$7) and header$7 and (s near2 box or (substitution near2 box))).clm.)	2
□	L35	(((scrambl$7) same (coded near4 video)) and (random near2 position))	0
□	L34	(((scrambl$7) same (coded near4 video)) and (random) and header)	9
□	L33	((scrambl$7 near6 random near6 position) same character$6)	2
□	L32	(MPEG and (substitution near2 table) and scrambl$8)	6
□	L31	mpeg and normalized and scrambl$8	347
□	L30	5600721 and random	13
□	L29	5600721.pn. and random	0
□	L28	20010050990	2
□	L27	L25 same mpeg and encrypt$7	11
□	L26	L25 same mpeg	14
□	L25	scrambl$7 near6 parameter$7	386
□	L24	L23 same character$6	2
□	L23	scrambl$7 near6 random near6 position	50
□	L22	scrambl$7 near6 random nrear6 position	7149203
□	L21	substitut$7 near7 random same video and scrambl$8	12
□	L20	substitut$7 near7 random same video andscrambl$8	72
□	L19	substitut$7 near7 random same video same scrambl$8	5
□	L18	substitut$7 near7 random same video	72

□	L8	arani and (partial and video)	3
□	L7	arani and (partial same video)	0
□	L6	arani and (partial same scrambl$7)	1
□	L5	arani and (partial same scrambl$&)	0
□	L4	video near2 scrambl$8 same partial	16
□	L3	10-145772	0
□	L2	145772	37
□	L1	6513122.pn.	3

END OF SEARCH HISTORY